Types of Malware

Malware is a term for *malicious software* designed to *disrupt computer systems*, *steal information,* or gain *unauthorized access*

Viruses

Computer viruses are *malicious programs* that can spread between computers and damage files.

1. **Propagation (Spread)**
2. **Effects**
3. **Prevention**

Viruses

1 Propagation (Spread)

Viruses *spread through infected files*, email attachments, and removable media.

2 Effects

- ✓ Viruses can ***cause da***
- ✓ **slow performance**
- ✓ **and system instabilit**

3 Prevention

- ✓ Use antivirus software,
- ✓ keep software updated,
- ✓ and be cautious about opening attachments from unknown sources.

Worms

Worms are self-replicating programs that can spread through networks without human interaction.

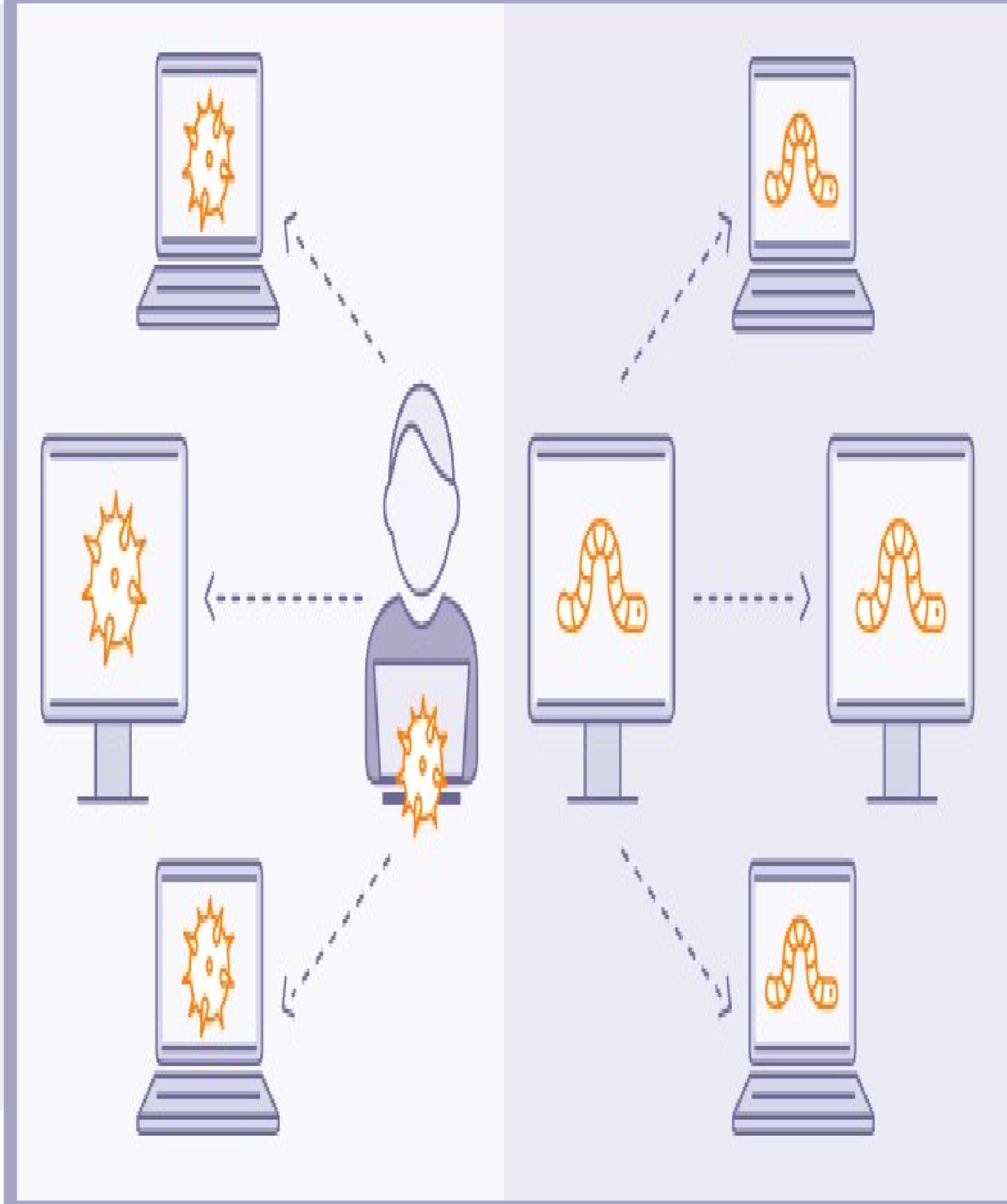
1 ***Replication***

2 ***Exploitation***

3 ***Impact***

1 *Replication*

Worms can replicate themselves and spread to other computers on a network.



Worms

2*Exploitation*

Worms exploit vulnerabilities in operating systems or applications to have access to systems.

Worms

3 *Impact*

Worms can cause network disruptions, data loss, and system interruptions

Trojans

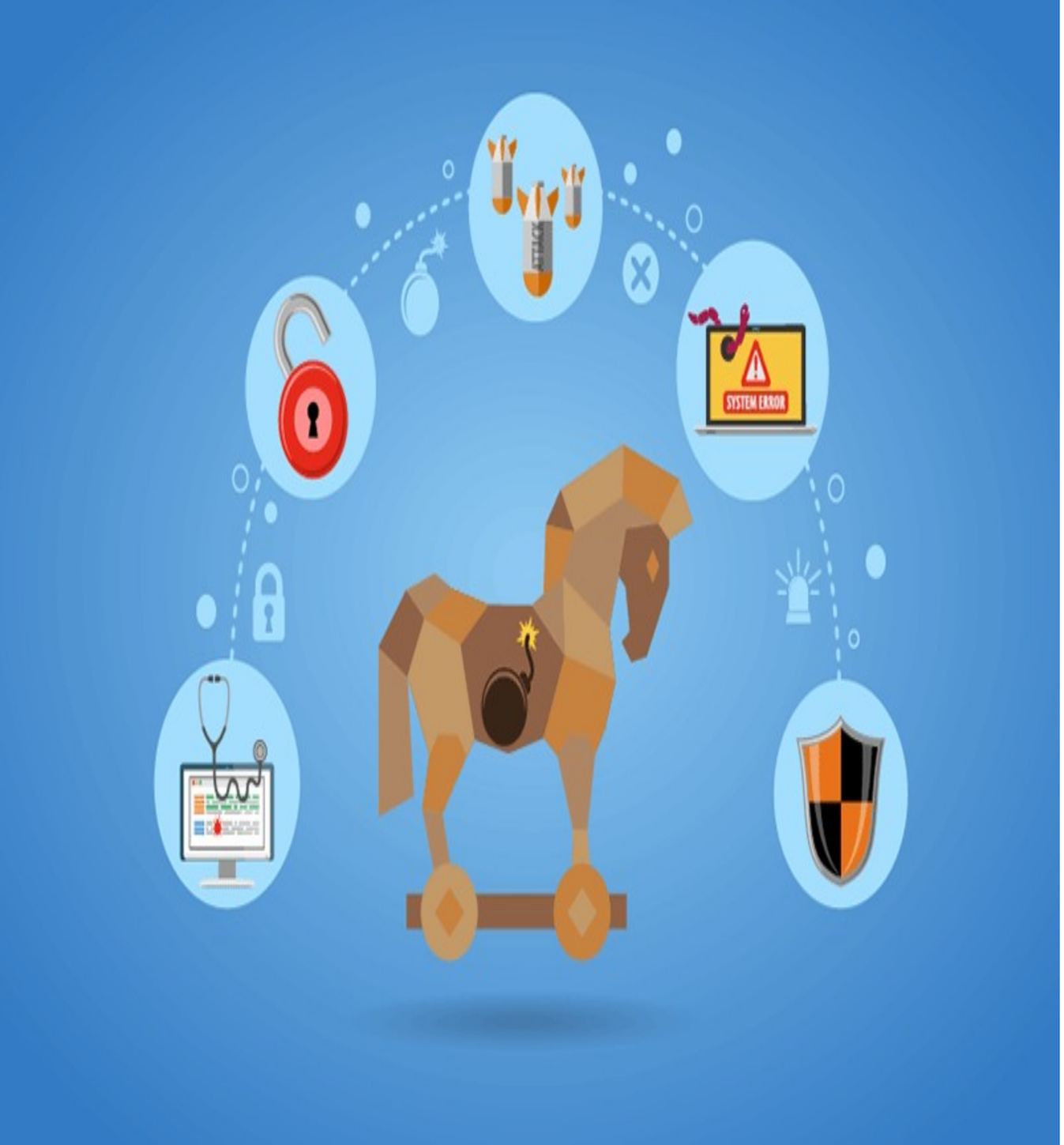
Trojans camouflage themselves as *legitimate software* but contain malicious code that can steal data, compromise systems, or provide remote access to attac

Camouflage ***Access*** ***Data Theft***

Trojans

Camouflage

Trojans can be disguised as games, utilities, or even software updates.



Trojans

Access

Trojans can provide attackers with unauthorized access to your computer or network.

Made with Gamma

Trojans

Data Stealing

Trojans can steal sensitive information, such as passwords, credit card details, and personal files.

Ransomware

Ransomware encrypts files on a computer and demands a ransom payment to decrypt them.

1. **Encryption**
2. **Demand**
3. **Decryption**

Ransomware

1

Encryption

Ransomware encrypts files

computer, making them inacces

Ransomware

Demand

Attackers demand a ransom payment to decrypt the files.

Ransomware

3

Decryption

Once the ransom is paid, attackers may or may not

Spyware

Spyware secretly monitors and collects information about your online activity, browsing history, and personal

Tracking

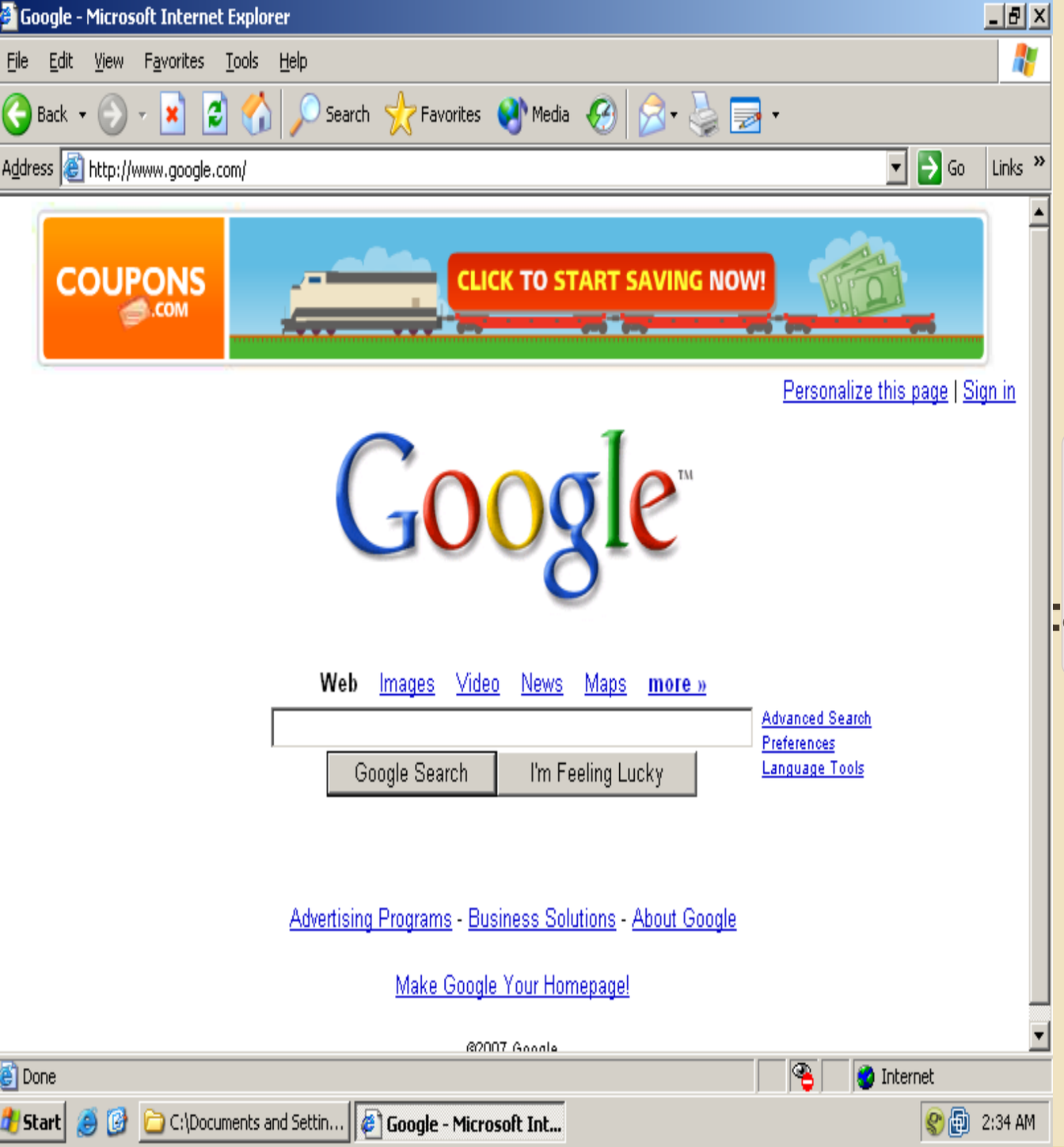
Advertising

Identity Theft

Spyware

Tracking

yware tracks your browsing activity
ystrokes, and personal information



Spyware

Advertising

Spyware can be used to display targeted advertising based on your browsing history.

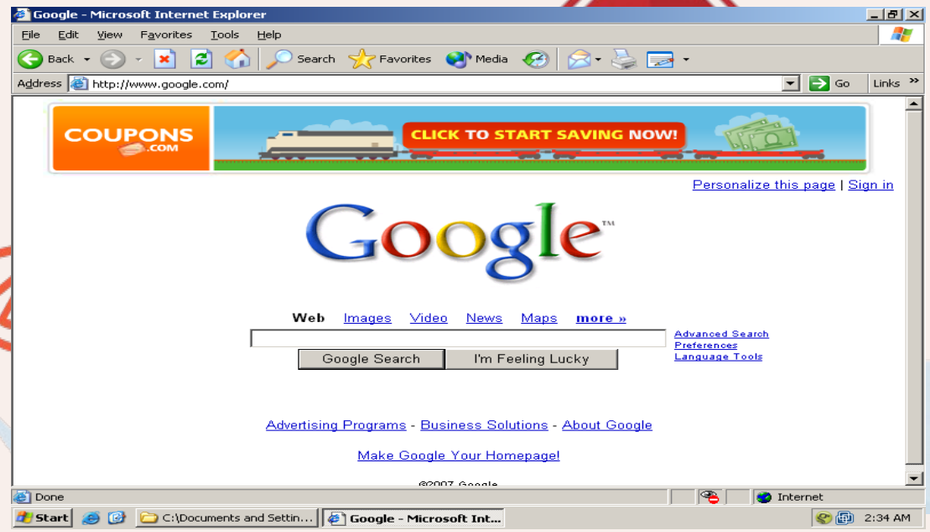
Spyware

Identity Theft

Spyware can be used to steal your personal information, such as passwords, credit card numbers, and bank account details.

Adware

Adware displays unwanted advertisements on your computer, often in the form of pop-ups or banners.



Type	***Description***
Pop-up Ads	**Ads that appear suddenly and unexpectedly on your screen.**
Banner Ads	**Ads that appear as horizontal banners at the top or bottom of a webpage.**
Contextual Ads	**Ads that are based on your browsing history and interests.**

Scareware

Scareware uses fraudulent tactics to scare users into downloading malicious software.
It typically displays fake security warnings or error messages.

Antivirus - Threaths detected
WARNING!
5 viruses detected!!
Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:
System crashing
Files deleted
Personal info stealing
Loss of Wi-Fi
Infecting your other devices
Remove viruses now
I don't want to be safe

Fake Security Alerts

Scareware displays fake security warnings or error messages to scare users into downloading malicious

Fraudulent Tactics

Scareware uses fraudulent tactics to trick users into downloading malicious software.

Rootkit

Rootkits are designed to hide their presence on a computer and provide attackers with persistent access. They can be used to steal data, control the system, or launch further attacks.

1 **Hidden**

Rootkits are designed to hide their presence from users and security software.

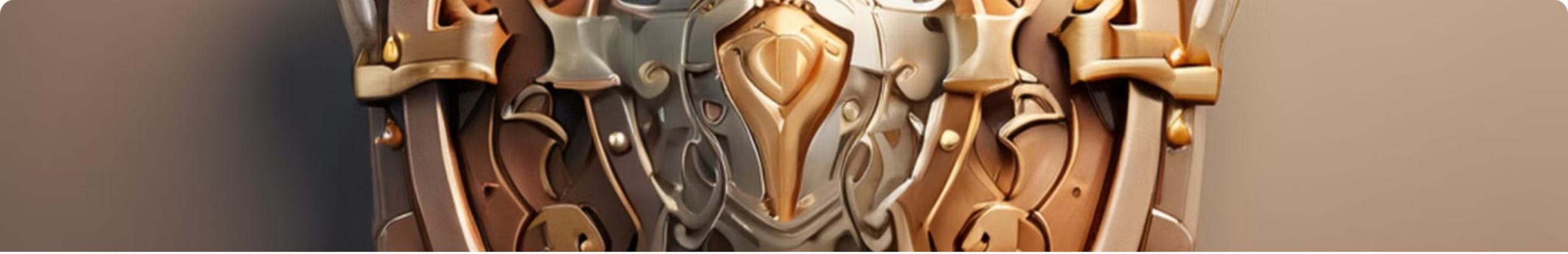
2 **Persistence**

Rootkits provide attackers with persistent access to a computer.

3 **Damage**

Rootkits can be used to steal data, control the system, or launch further attacks.

Made with Gamma



Preventive Measures

To protect your computer, you have to use several defenses. including using antivirus software, keeping your system updated, and practicing safe browsing habits.

Antivirus Software

Install and keep your antivirus software up-to-date to detect and remove malware.

Strong Passwords

Use strong, unique passwords for all your online accounts.

Software Updates

Install software updates regularly to patch security vulnerabilities.

Safe Browsing

Be cautious about clicking on suspicious links, opening attachments from unknown sources, and downloading files from untrusted websites.